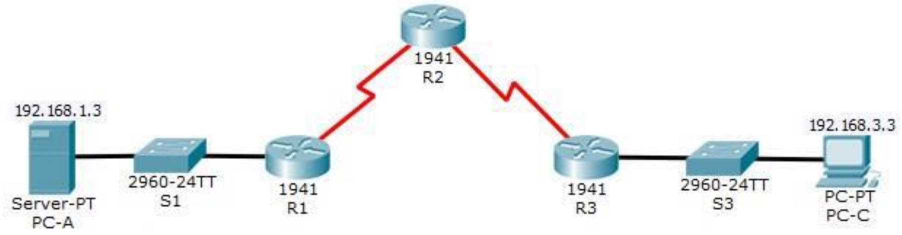
UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

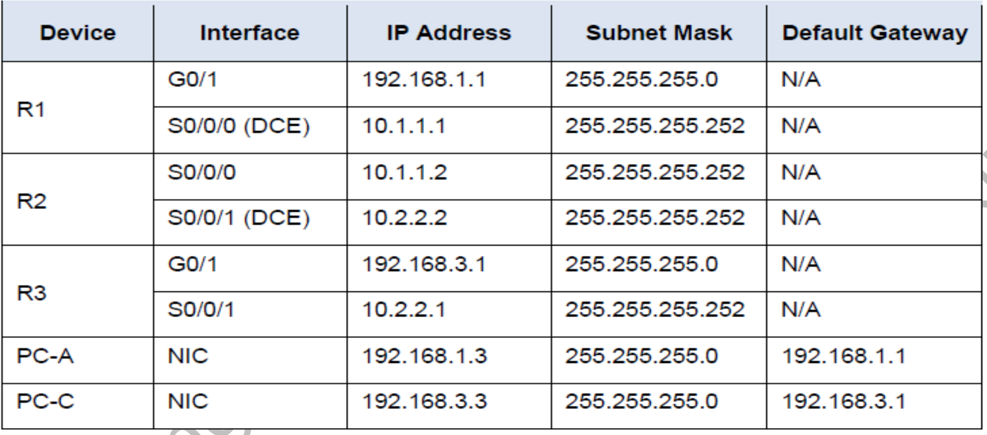
1

Seat No: ____________ **Max. Marks: 50**

1.	Create the following topology	**20**



Addressing table



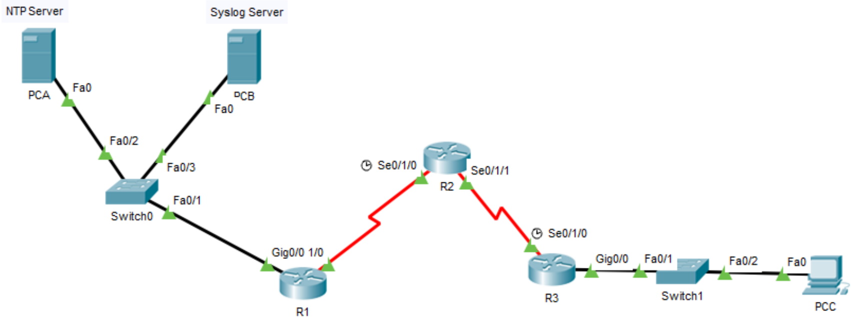
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

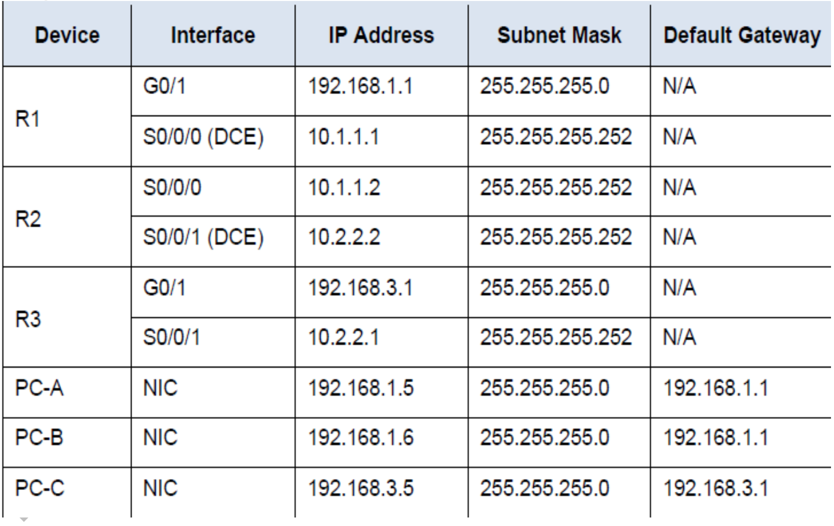
2.	Configure a zone-based policy (ZPF) firewall on R3.	**10**
3.	Verify ZPF firewall functionality using ping, SSH, and a web browser.	**10**
4.	Viva	**5**
5.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

2

Seat No: ____________ **Max. Marks: 50**

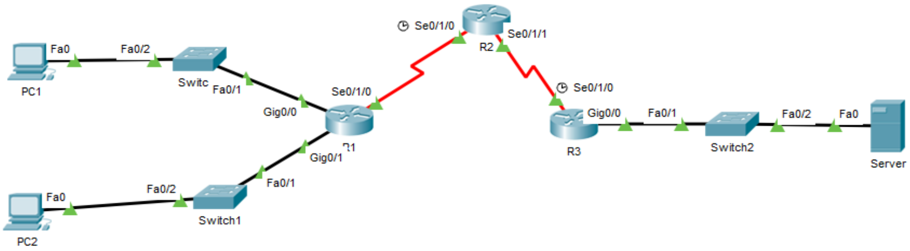
<table>
<tr><td>1.</td><td>Create the following topology


Addressing Table

<table>
<tr><th>Device</th><th>Interface</th><th>IP Address</th><th>Subnet Mask</th><th>Default Gateway</th></tr>
<tr><td>R1</td><td>G0/1</td><td>192.168.1.1</td><td>255.255.255.0</td><td>N/A</td></tr>
<tr><td></td><td>S0/0/0 (DCE)</td><td>10.1.1.1</td><td>255.255.255.252</td><td>N/A</td></tr>
<tr><td>R2</td><td>S0/0/0</td><td>10.1.1.2</td><td>255.255.255.252</td><td>N/A</td></tr>
<tr><td></td><td>S0/0/1 (DCE)</td><td>10.2.2.2</td><td>255.255.255.252</td><td>N/A</td></tr>
<tr><td>R3</td><td>G0/1</td><td>192.168.3.1</td><td>255.255.255.0</td><td>N/A</td></tr>
<tr><td></td><td>S0/0/1</td><td>10.2.2.1</td><td>255.255.255.252</td><td>N/A</td></tr>
<tr><td>PC-A</td><td>NIC</td><td>192.168.1.5</td><td>255.255.255.0</td><td>192.168.1.1</td></tr>
<tr><td>PC-B</td><td>NIC</td><td>192.168.1.6</td><td>255.255.255.0</td><td>192.168.1.1</td></tr>
<tr><td>PC-C</td><td>NIC</td><td>192.168.3.5</td><td>255.255.255.0</td><td>192.168.3.1</td></tr>
</table></td><td>**20**</td></tr>
<tr><td>2.</td><td>Configure OSPF MD5 authentication.</td><td>**10**</td></tr>
<tr><td>3.</td><td>Configure NTP and configure routers to log messages to the Syslog Server</td><td>**10**</td></tr>
<tr><td>4.</td><td>Viva</td><td>**5**</td></tr>
<tr><td>5.</td><td>Journal</td><td>**5**</td></tr>
</table>

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ___________ **Max. Marks: 50**

1. Create the following topology **20**



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
PC1	NIC	2001:DB8:1:10::10/64	FE80::1
PC2	NIC	2001:DB8:1:11::11/64	FE80::1
R1	Gig0/0	2001:DB8:1:10::1/64	FE80::1
	Gig0/1	2001:DB8:1:11::1/64	FE80::1
	Se0/1/0	2001:DB8:1:1::1/64	FE80::1
R2	Se0/1/0	2001:DB8:1:1::2/64	FE80::2
	Se0/1/1	2001:DB8:1:2::2/64	FE80::2
R3	Gig0/0	2001:DB8:1:30::1/64	FE80::3
	Se0/1/0	2001:DB8:1:2::1/64	FE80::3
Server	NIC	2001:DB8:1:30::30/64	FE80::3

2. Configure ,apply and verify an ACL that will block HTTP and HTTPS access on R1 **20**

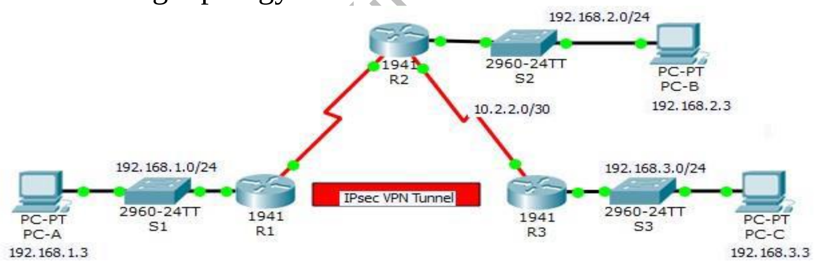
3. Viva **5**

4. Journal **5**

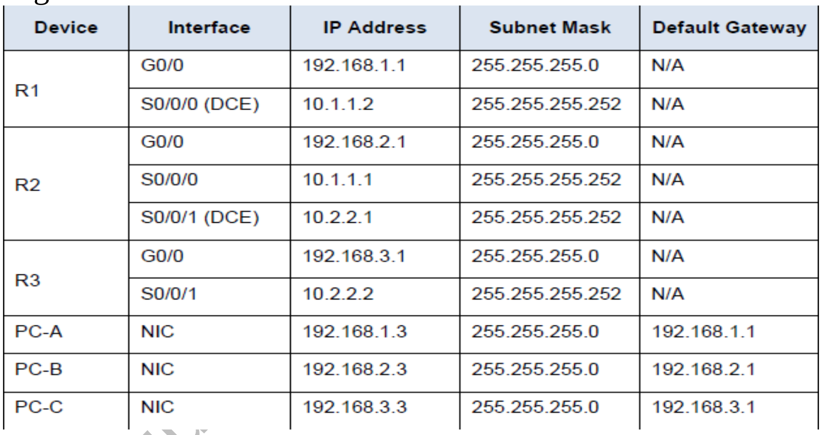
UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ___________ **Max. Marks: 50**

1. Create the following topology **20**



Addressing Table



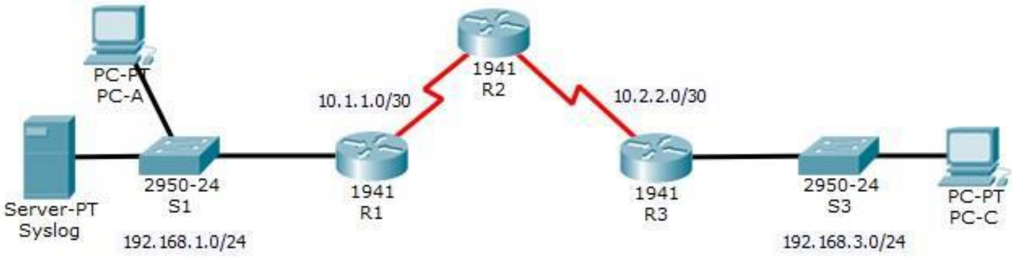
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

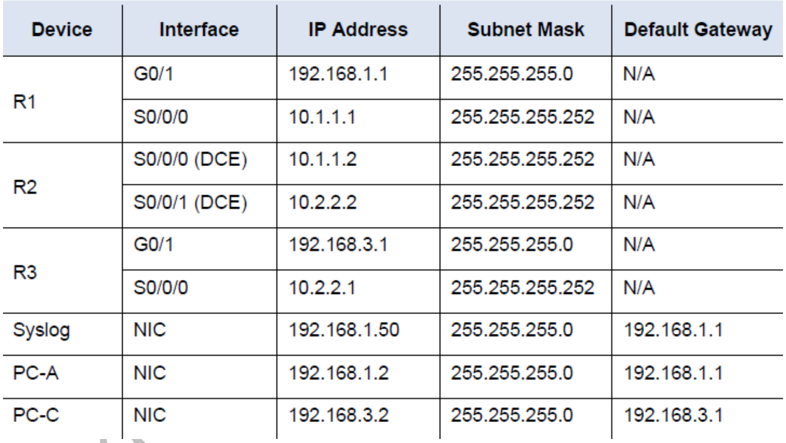
2.	Configure and verify R1 to support a site-to-site IPsec VPN with R3.	**20**
3.	Viva	**5**
4.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

5

Seat No: ___________ **Max. Marks: 50**

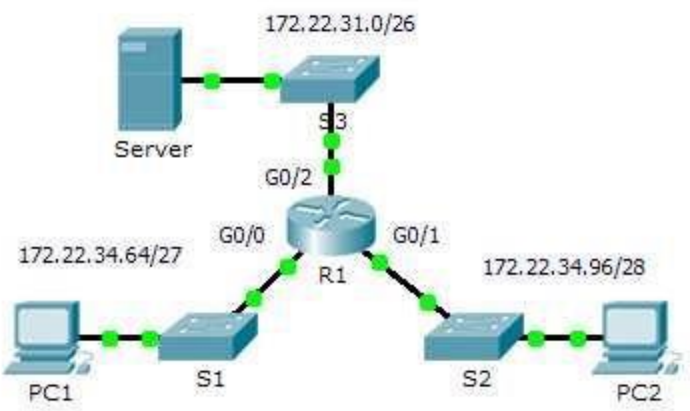
<table>
<tr><td>1.</td><td>Create the following topology


Addressing Table

<table>
<tr><th>Device</th><th>Interface</th><th>IP Address</th><th>Subnet Mask</th><th>Default Gateway</th></tr>
<tr><td>R1</td><td>G0/1</td><td>192.168.1.1</td><td>255.255.255.0</td><td>N/A</td></tr>
<tr><td></td><td>S0/0/0</td><td>10.1.1.1</td><td>255.255.255.252</td><td>N/A</td></tr>
<tr><td>R2</td><td>S0/0/0 (DCE)</td><td>10.1.1.2</td><td>255.255.255.252</td><td>N/A</td></tr>
<tr><td></td><td>S0/0/1 (DCE)</td><td>10.2.2.2</td><td>255.255.255.252</td><td>N/A</td></tr>
<tr><td>R3</td><td>G0/1</td><td>192.168.3.1</td><td>255.255.255.0</td><td>N/A</td></tr>
<tr><td></td><td>S0/0/0</td><td>10.2.2.1</td><td>255.255.255.252</td><td>N/A</td></tr>
<tr><td>Syslog</td><td>NIC</td><td>192.168.1.50</td><td>255.255.255.0</td><td>192.168.1.1</td></tr>
<tr><td>PC-A</td><td>NIC</td><td>192.168.1.2</td><td>255.255.255.0</td><td>192.168.1.1</td></tr>
<tr><td>PC-C</td><td>NIC</td><td>192.168.3.2</td><td>255.255.255.0</td><td>192.168.3.1</td></tr>
</table>
</td><td><b>20</b></td></tr>
<tr><td>2.</td><td>Enable IOS IPS</td><td><b>10</b></td></tr>
<tr><td>3.</td><td>Configure logging and verify IPS</td><td><b>10</b></td></tr>
<tr><td>4.</td><td>Viva</td><td><b>5</b></td></tr>
<tr><td>5.</td><td>Journal</td><td><b>5</b></td></tr>
</table>

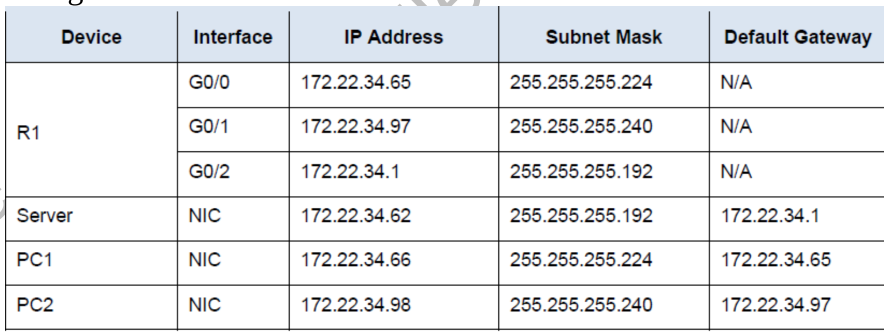
UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ___________ **Max. Marks: 50**

1.	Create the following topology	**20**



Addressing Table



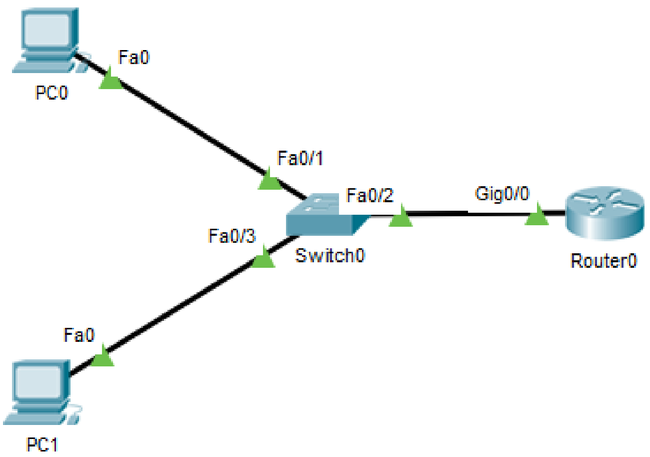
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

2.	Configure an ACL that will permit FTP and HTTP access on R1.	**10**
3.	Verify the ACL implementation. PC1 (Only FTP). PC2(Only HTTP)	**10**
4.	Viva	**5**
5.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ___________ **Max. Marks: 50**

<table>
<tr><td>1.</td><td>Create the following topology

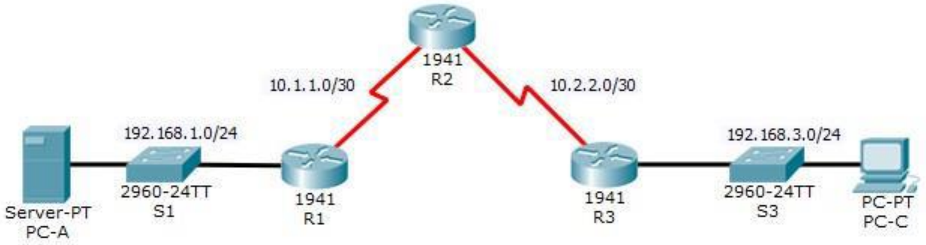


Addressing Table
<table>
<tr><th>Device</th><th>Interface</th><th>IP Address</th><th>Subnet Mask</th><th>Default Gateway</th></tr>
<tr><td>R1</td><td>Gig0/0</td><td>192.168.1.1</td><td>255.255.255.0</td><td>N/A</td></tr>
<tr><td>PC0</td><td>NIC</td><td>192.168.1.2</td><td>255.255.255.0</td><td>192.168.1.1</td></tr>
<tr><td>PC1</td><td>NIC</td><td>192.168.1.3</td><td>255.255.255.0</td><td>192.168.1.1</td></tr>
</table>
</td><td><b>20</b></td></tr>
<tr><td>2.</td><td>Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.</td><td><b>10</b></td></tr>
<tr><td>3.</td><td>Verify local AAA authentication from the R1 console and the PC0 client and PC1 Client.</td><td><b>10</b></td></tr>
<tr><td>4.</td><td>Viva</td><td><b>5</b></td></tr>
<tr><td>5.</td><td>Journal</td><td><b>5</b></td></tr>
</table>

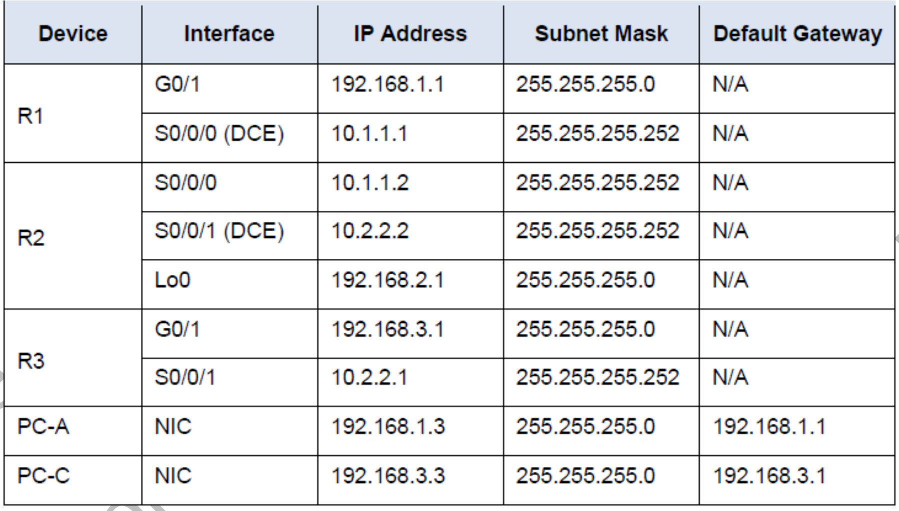
UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ___________ **Max. Marks: 50**

1. Create the following topology **20**



Addressing Table



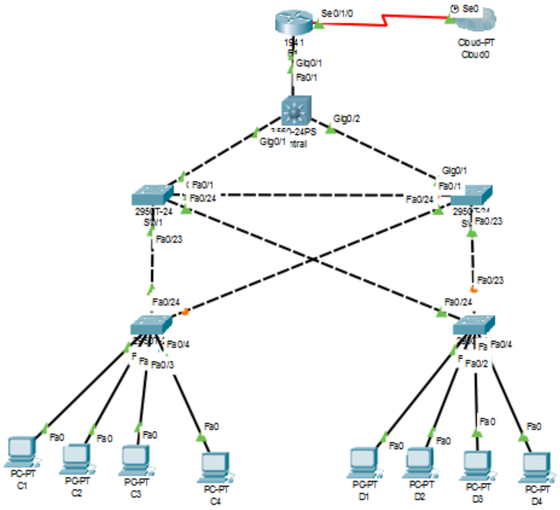
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

2.	Configure ACL to allow access to routers R1, R2, and R3 to only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, which is a server providing DNS, SMTP, FTP, and HTTPS services.	**10**
3.	Verify ACL functionality	**10**
4.	Viva	**5**
5.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ____________ **Max. Marks: 50**

1. Create the following topology **10**



Addressing Table

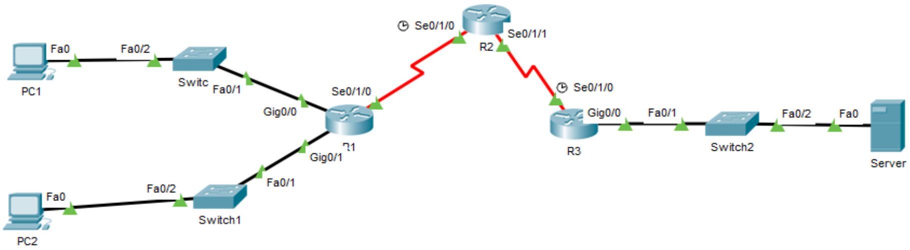
Devices	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gig0/1	192.168.1.1	255.255.255.0	N/A
	Se0/0/0	209.165.200.1	255.255.255.0	N/A
C1	NIC	10.1.1.10	255.255.255.0	10.1.1.1
C2	NIC	10.1.1.11	255.255.255.0	10.1.1.1
C3	NIC	10.1.1.12	255.255.255.0	10.1.1.1
C4	NIC	10.1.1.13	255.255.255.0	10.1.1.1
D1	NIC	10.1.1.14	255.255.255.0	10.1.1.1
D2	NIC	10.1.1.15	255.255.255.0	10.1.1.1
D3	NIC	10.1.1.16	255.255.255.0	10.1.1.1
D4	NIC	10.1.1.17	255.255.255.0	10.1.1.1

2.	Assign the Central switch as the root bridge.	**10**
3.	Secure spanning-tree parameters to prevent STP manipulation attacks.	**10**
4.	Enable port security to prevent CAM table overflow attacks.	**10**
5.	Viva	**5**
6.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ____________ **Max. Marks: 50**

1.	Create the following topology	**20**



Addressing Table

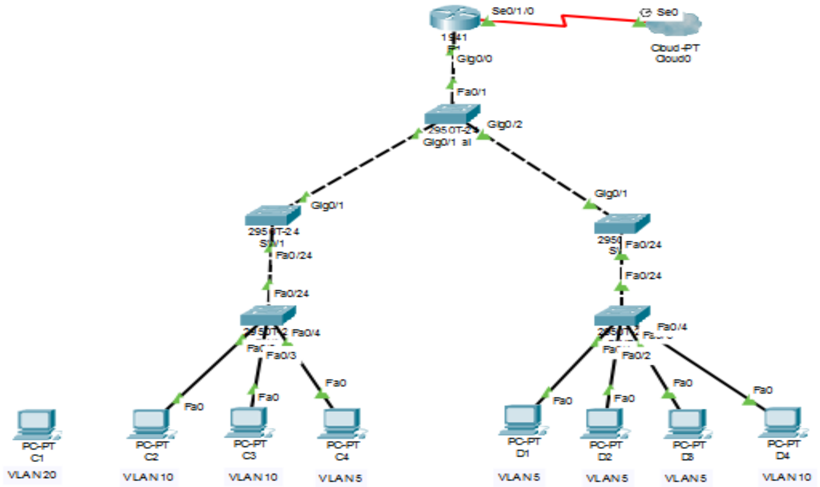
Device	Interface	IPv6 Address/Prefix	Default Gateway
PC1	NIC	2001:DB8:1:10::10/64	FE80::1
PC2	NIC	2001:DB8:1:11::11/64	FE80::1
R1	Gig0/0	2001:DB8:1:10::1/64	FE80::1
	Gig0/1	2001:DB8:1:11::1/64	FE80::1
	Se0/1/0	2001:DB8:1:1::1/64	FE80::1
R2	Se0/1/0	2001:DB8:1:1::2/64	FE80::2
	Se0/1/1	2001:DB8:1:2::2/64	FE80::2
R3	Gig0/0	2001:DB8:1:30::1/64	FE80::3
	Se0/1/0	2001:DB8:1:2::1/64	FE80::3
Server	NIC	2001:DB8:1:30::30/64	FE80::3

2.	Configure, apply and verify an ACL that will block ICMP access on R3	**20**
3.	Viva	**5**
4.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ____________ **Max. Marks: 50**

1.	Create the following topology	**20**



Addressing Table

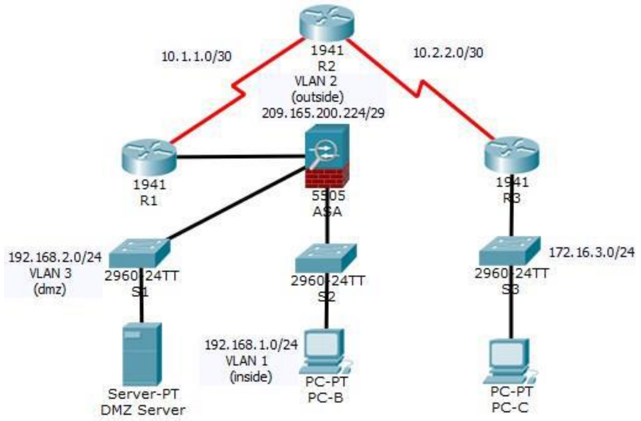
Devices	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gig0/1			
	Se0/0/0	209.165.200.1	255.255.255.0	N/A
C2	NIC	192.168.10.1	255.255.255.0	192.168.10.100
C3	NIC	192.168.10.2	255.255.255.0	192.168.10.100
C4	NIC	192.168.5.1	255.255.255.0	192.168.5.100
D1	NIC	192.168.5.2	255.255.255.0	192.168.5.100
D2	NIC	192.168.5.3	255.255.255.0	192.168.5.100
D3	NIC	192.168.5.4	255.255.255.0	192.168.5.100
D4	NIC	192.168.10.3	255.255.255.0	192.168.10.100

2.	Enable trunking and configure security on the trunk link.	**10**
3.	Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN. Verify connectivity of the management PC to all switches.	**10**
4.	Viva	**5**
5.	Journal	**5**

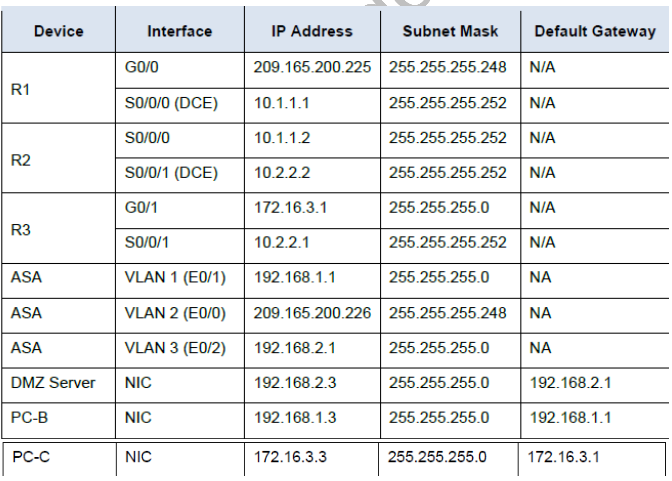
UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

Seat No: ____________ **Max. Marks: 50**

1.	Create the following topology	**20**



Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

2.	Configure basic ASA settings and interface security levels using CLI	**10**
3.	Configure routing, address translation, and inspection policy using CLI. Test connectivity to the ASA.	**10**
4.	Viva	**5**
5.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

13

Seat No: ___________ **Max. Marks: 50**

1.	For the given topology (Exam1.pkt) a) Configure OSPF MD5 authentication b) Configure NTP and configure routers to log messages to the Syslog Server	**20**
2.	For the given topology (Exam3.pkt) a) Enable trunking and configure security on the trunk line. b) Verify connectivity between VLAN10 and VLAN20	**20**
3.	Viva	**5**
4.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

14

Seat No: ___________ **Max. Marks: 50**

1.	For the given topology (Exam4.pkt) a) Configure ACL to allow access to routers R1, R2, and R3 to only be permitted from PC0, the management station. PC0 is also used for connectivity testing to Server0, which is a server providing DNS and HTTPS services.	**20**
2.	For the given topology (Exam8.pkt) a) PC0 needs web access and PC1 needs FTP access provided by the server. b) Both computers are able to ping the server but not each other. c) Configure, apply and verify the ACL.	**20**
3.	Viva	**5**
4.	Journal	**5**

UNIVERSITY OF MUMBAI

T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)

(Practical Examination)

SECOND HALF 2019

SUBJECT: SECURITY IN COMPUTING

15

(SUBJECT CODE: USIT6P2)

Seat No: ____________ **Max. Marks: 50**

1.	For the given topology (Exam4.pkt) a) Configure ACL to allow access to routers R1, R2, and R3 to only be permitted from PC0, the management station. PC0 is also used for connectivity testing to Server0, which is a server providing SMTP and FTP services.	**20**
2.	3. For the given topology (Exam1.pkt) a) Configure NTP and configure routers to log messages to the Syslog Server b) Configure R4 to support SSH connection.	**20**
4.	Viva	**5**
5.	Journal	**5**

UNIVERSITY OF MUMBAI

T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)

(Practical Examination)

SECOND HALF 2019

SUBJECT: SECURITY IN COMPUTING

(SUBJECT CODE: USIT6P2)

16

Seat No: ____________ **Max. Marks: 50**

1.	For the given topology (Exam5.pkt) a) Enable IPS on R1 to scan traffic entering 192.168.1.0 network. Configure the router to identify the syslog server to receive logging messages by displaying correct time and date in messages. b) Enable IPS to produce alert and drop ICMP echo reply packets inline.	**20**
2.	For the given topology (Exam6.pkt) a) Assign central switch as root bridge b) Secure spanning-tree parameters to prevent STP manipulation attacks c) Enable port security to prevent CAM overflow attacks	**20**
3.	Viva	**5**
4.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

17

Seat No: ___________ **Max. Marks: 50**

1.	For the given topology (Exam4.pkt) a) Configure a zone-based policy (ZPF) firewall on R1. b) Verify ZPF firewall functionality using ping, SSH, and a web browser	**20**
2.	For the given topology (Exam3.pkt) a) Enable trunking and configure security on the trunk line. b) Verify connectivity between VLAN10 and VLAN20	**20**
3.	Viva	**5**
4.	Journal	**5**

UNIVERSITY OF MUMBAI
T.Y.B.Sc. INFORMATION TECHNOLOGY (Semester VI)
(Practical Examination)
SECOND HALF 2019
SUBJECT: SECURITY IN COMPUTING
(SUBJECT CODE: USIT6P2)

18

Seat No: ___________ **Max. Marks: 50**

1.	For the given topology (Exam7.pkt) a) Configure devices on one LAN to remotely access devices in another LAN using the SSH protocol. b) Besides ICMP, all traffic should be denied.	**20**
2.	For the given topology (Exam2.pkt) a) Configure a local user account on R1 and R2 and configure authentication on the console and vty lines using local AAA. b) Verify local AAA authentication from the R1 and R2 console on PC0 client and PC1 Client	**20**
3.	Viva	**5**
4.	Journal	**5**